

On values of binary quadratic forms at integer points

Manoj Choudhuri and S. G. Dani

Abstract

We obtain estimates for the number of integral solutions in large balls, of inequalities of the form $|Q(x, y)| < \epsilon$, where Q is an indefinite binary quadratic form, in terms of the Hurwitz continued fraction expansions of the slopes of the lines on which Q vanishes. The method is based on a coding of geodesics on the modular surface via Hurwitz expansions of the endpoints of their lifts in the Poincaré half-plane.

1 Introduction

Consider a binary quadratic form $Q(x, y) = (ax + by)(cx + dy)$, where $a, b, c, d \in \mathbb{R}$ and $ad - bc \neq 0$. In this paper we exhibit a close relationship between the growth of the number of solutions (x, y) , with $x, y \in \mathbb{Z}$, with $\gcd(|x|, |y|) = 1$, of

$$|Q(x, y)| < \epsilon \quad \text{and} \quad \|(x, y)\| \leq \rho, \quad (1)$$

asymptotically as $\rho \rightarrow \infty$ and the continued fraction expansions of a/b and c/d with respect to the Hurwitz algorithm (see below for details), when at least one of the ratios are irrational. Here and in the sequel $\|\cdot\|$ stands for the Euclidean norm on \mathbb{R}^2 . For any set E we shall denote by $\#E$ the cardinality of E .

We recall (see [3] for instance) that any irrational number ξ can be expressed as

$$\xi = a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \dots}},$$

with $a_j \in \mathbb{Z}$ and (i) $|a_j| \geq 2$ for all j and if (ii) $|a_j| = 2$ for some j then $a_j a_{j+1} < 0$ (i.e. if $|a_j| = 2$ then a_j and a_{j+1} have the opposite sign); here the right hand side stands, as usual, for the limit (with existence assured) of the sequence of rational numbers represented by terms of corresponding to the truncated expressions. We draw the reader's attention to that in writing the expression as above the successive terms are subtracted, rather than added; this is often done in literature (see [3] for

instance) on account of its being in consonance with the action of the modular group; an expansion as above is called the *minus continued fraction expansion* with respect to the nearest integer algorithm (or also as the Hurwitz algorithm). We shall, as usual, denote the expression on the right hand side by $[a_0, a_1, \dots]$. We recall also that, conversely, given a sequence $\{a_j\}$ of integers satisfying conditions (i) and (ii) as above there is a unique irrational number ξ such that $\xi = [a_0, a_1, \dots]$.

We recall that an integral pair (x, y) is said to be *primitive* if it is nonzero and $\frac{1}{k}(x, y)$ is not an integral pair for any natural number k ; in other words, if $(x, y) \neq (0, 0)$ and $\gcd(|x|, |y|) = 1$. In the sequel we denote by \mathfrak{p} the set of all primitive integral pairs.

We shall be interested in primitive solutions of inequalities as in (1), with $Q(x, y) = (ax + by)(cx + dy)$, where we assume the ratio a/b to be irrational. It will be convenient to consider primitive solutions in the region defined by

$$\{(x, y) : 0 < Q(x, y) < \delta, \quad cx + dy > \kappa \quad \text{and} \quad \|(x, y)\| \leq \rho\}, \quad (2)$$

with $\kappa > 0$, as indicated by the shaded region in Figure 1; estimates for the number of primitive integral solutions to inequalities as in (1) can then be obtained by putting together the solutions in various subregions (from various tentacles as in Figure 1); see Remark 1.4 for details. Theorem 1.1 below addresses this in terms of the minus continued fraction of a/b , giving lower and upper estimates for the number of solutions when ρ is sufficiently large. We mention here that in the course of the proof a more concrete relationship is proved for a special class of quadratic forms called *H-reduced* forms (see §4 for definition of *H-reduced*, and Theorem 4.1 for the result involved). It may also be noted that a somewhat sharper, but more technical, version of the following theorem may be contained in Corollary 5.1; the various constants involved are also given in sharper form in the latter.

Theorem 1.1. *Let $Q(x, y) = (ax + by)(cx + dy)$ be a quadratic form, where $a, b, c, d \in \mathbb{R}$, $ad - bc = 1$, $b \neq 0$ and $\frac{a}{b}$ is irrational. Let $[a_0, a_1, \dots]$ be the minus continued fraction expansion of $\frac{a}{b}$. Let*

$$\alpha^- = \liminf \frac{1}{n} \sum_{j=0}^{n-1} \log |a_j| \quad \text{and} \quad \alpha^+ = \limsup \frac{1}{n} \sum_{j=0}^{n-1} \log |a_j|.$$

Let $0 < \delta < \frac{1}{\pi}$ and let $e(\delta)$ and $f(\delta)$ respectively denote the (asymptotic) lower density of $\{j \geq 0 \mid |a_j| \geq 2\delta^{-1} + 1\}$ and the upper density of $\{j \geq 0 \mid |a_j| \geq 2\delta^{-1} - \frac{3}{2}\}$. Let $\kappa > 0$ be fixed and let

$$R = \{(x, y) \in \mathbb{R}^2 \mid 0 < Q(x, y) < \delta, \quad cx + dy > \kappa\}.$$

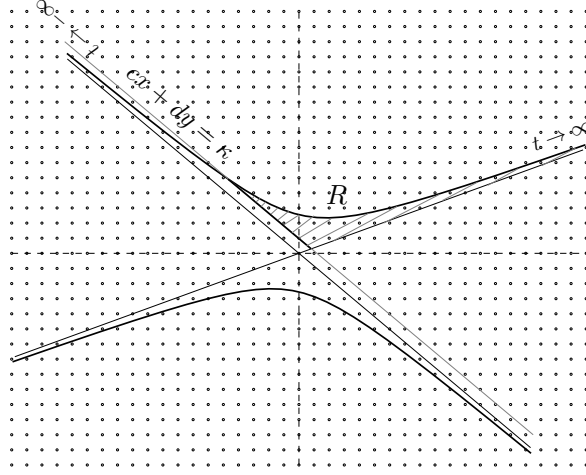


Figure 1: The region R

For any $\rho > 0$ let

$$G(\rho) = \{(x, y) \in \mathfrak{p} \cap R \mid \|(x, y)\| \leq \rho\}.$$

Then we have the following :

i) if $\alpha^+ < \infty$ then there exists ρ_0 such that for all $\rho \geq \rho_0$ we have

$$\#G(\rho) \geq \frac{e(\delta)}{(\alpha^+ + 3)} \log \rho;$$

ii) given $m > f(\delta)$, and $M \geq \frac{1}{4} \log \frac{9}{5}$ such that $M < \frac{1}{8} \alpha^-$ if $\alpha^- > 2 \log \frac{9}{5}$, there exists ρ_0 such that for all $\rho \geq \rho_0$ we have

$$\#G(\rho) \leq \frac{m}{M} \log \rho;$$

(if α^- is infinite, the assertion holds for all positive M).

Remark 1.2. The assertion in (ii) shows in particular that for any quadratic form Q as in Theorem 1.1 and $0 < \delta < \frac{1}{\pi}$, such that for all sufficiently large ρ we have $\#G(\rho) \leq (\frac{1}{4} \log \frac{9}{5}) \log \rho$. The area of the of the region $R \cap B(\rho)$, where $B(\rho) = \{(x, y) \mid \|(x, y)\| \leq \rho\}$, R is as in the theorem and for some choice of $\kappa > 0$, is asymptotic to $\log \rho$, and the preceding observation signifies that the the number of primitive integral pairs in $R \cap B(\rho)$ is bounded, for all large ρ , by a fixed multiple of the area of the region. We note that this contrasts the situation for linear forms in place of the quadratic forms where the number of primitive integral points in analogously defined regions can be arbitrarily large in proportion to the area of the region, depending on the linear form, on account of existence of very well approximable numbers. We may also mention here the following, concerning quadratic forms in higher number of

variables. For all nondegenerate indefinite, irrational (not a scalar multiple of a form with rational coefficients) forms in $n \geq 3$ variables such a ratio is bounded below and for $n \geq 5$ the ratio converges to 1; for $n = 3$ or 4 there are counter-examples to the second part; see [5] for details.

Remark 1.3. Let Q be the quadratic form as in Theorem 1.1 such that both a/b and c/d are irrational. Let $0 < \delta < \frac{1}{\pi}$ and for any $\rho > 0$ let

$$H(\rho) = \{(x, y) \in \mathfrak{p} \mid 0 < Q(x, y) < \delta \text{ and } \|(x, y)\| \leq \rho\}, \text{ and}$$

$$G'(\rho) = \{(x, y) \in \mathfrak{p} \mid 0 < Q(x, y) < \delta, ax + by > \sqrt{\delta} \text{ and } \|(x, y)\| \leq \rho\}.$$

Then for any $\rho > 0$ we have that $\#H(\rho)$ differs from $2(\#G(\rho) + \#G'(\rho))$ by at most 2, as maybe observed from Figure 1; note that here κ is chosen to be $\sqrt{\delta}$. Also, $\#G'(\rho)$ admits analogous estimates as $\#G(\rho)$ with the continued fraction expansion of c/d in place of a/b . Thus the theorem provides estimates for $\#H(\rho)$ under appropriate conditions as in the hypothesis of the theorem.

Remark 1.4. It may be emphasized that Theorem 1.1 applies to *all* irrational numbers α ; thus, given any sequence $\{a_j\}$ with $a_j \in \mathbb{Z}$ such that $|a_j| \geq 2$ for all j and $a_j a_{j+1} < 0$ if $|a_j| = 2$ we have an irrational number $\alpha = [a_0, a_1, \dots]$ and a corresponding result for any $c, d \in \mathbb{R}$ such that $ad - bc = 1$. One may ask what the typical, or generic, values of the constants involved are. Specifically the question may be formulated as follows. As in the case of the usual continued fractions there is a corresponding Gauss map associated to the minus continued fraction, defined on $I = [-\frac{1}{2}, \frac{1}{2}] \setminus \mathbb{Q}$, by $T(x) = -\frac{1}{x} + \nu(x)$, where $\nu(x)$ denotes the integer nearest to x . The Gauss measure in the usual case also has an analogue, and is given by $\mu(E) = c \int_I \frac{1}{4-x^2} dx$, where $c > 0$ is the normalising constant (see [4], §6). The measure μ is ergodic with respect to T ; this can be proved along the lines of the arguments for the case of simple continued fractions, say as in [1], and we shall not go into the details here. The ergodicity implies that for almost all $\alpha = [a_0, a_1, \dots]$, $\frac{1}{n} \sum_{j=0}^{n-1} \log |a_j|$ converges to $\int f d\mu$, where $f : I \rightarrow (0, \infty)$ is the function defined by $f(x) = \log |a|$ if either $x \in \left(\frac{1}{a+\frac{1}{2}}, \frac{1}{a-\frac{1}{2}}\right)$ for $a > 0$ or $x \in \left(\frac{1}{a-\frac{1}{2}}, \frac{1}{a+\frac{1}{2}}\right)$ for $a < 0$ (see the proof of (3.26) in [1]); we note that f is integrable and $\int f d\mu$ is a positive constant; this constant then is the generic value of α^+ and α^- as in the statement of the theorem. Similarly, for a $\delta > 0$ the generic values of $e(\delta)$ and $f(\delta)$ are seen to $\mu([- \frac{1}{k}, \frac{1}{k}])$ and $\mu([- \frac{1}{l}, \frac{1}{l}])$ respectively, where $k = [2\delta^{-1} + 1]$ and $l = [2\delta^{-1} - \frac{3}{2}]$.

2 A correspondence

Let $G = SL(2, \mathbb{R})$. We denote by $\{e_1, e_2\}$ the standard basis of \mathbb{R}^2 . Let Q_0 be the quadratic form on \mathbb{R}^2 defined by $Q_0(xe_1 + ye_2) = xy$ for all $x, y \in \mathbb{R}$. For $g \in G$ we denote by Q_g the quadratic form defined by $Q_g(v) = Q_0(g^{-1}v)$ for all $v \in \mathbb{R}^2$.

For $t \in \mathbb{R}$ we denote by a_t the matrix $\text{diag}(e^{t/2}, e^{-t/2}) \in G$. For $g \in G$ and $t \in \mathbb{R}$, if $g_t = ga_tg^{-1}$, then for any $v \in \mathbb{R}^2$ we have $Q_g(g_tv) = Q_0(g^{-1}g_tv) = Q_0(a_tg^{-1}v) = Q_0(g^{-1}v) = Q_g(v)$; thus $\{g_t\}_{t \in \mathbb{R}}$ is contained in $SO(Q)$, and in fact coincides, by dimension considerations, with $SO(Q)^+$, the connected component of the identity in $SO(Q)$. In particular $\{v \in \mathbb{R}^2 \mid Q_g(v) \neq 0\}$ is $\{g_t\}$ -invariant. We note that in each connected component of $\{v \in \mathbb{R}^2 \mid Q_g(v) \neq 0\}$ the orbits of $\{g_t\}_{t \in \mathbb{R}}$ are the level curves of Q_g and they are asymptotic to the pair of lines defined by $Q_g(v) = 0$. We denote by L_g^+ and L_g^- the linear forms on \mathbb{R}^2 such that $Q_g = L_g^+ L_g^-$ and the level curves of Q_g , viewed as orbits of $\{g_t\}$, are asymptotic to $L_g^+(v) = 0$ as $t \rightarrow \infty$ and $L_g^-(v) = 0$ as $t \rightarrow -\infty$; see Figure 1.

Through the rest of the section we fix a $g \in G$ and let $Q = Q_g$. It may be mentioned that the results will have nontrivial content only when at least one of L_g^+ and L_g^- is not a rational form, but we make no specific assumption in this respect. Let $g_t = ga_tg^{-1}$ for all $t \in \mathbb{R}$. For any $v \in \mathbb{R}^2$ and any subset C of \mathbb{R}^2 we define

$$I_v(C) = \{t \geq 0 \mid v \in g_t C\} \text{ and } R(C) = \bigcup_{p \in \mathbb{Z}^2 \setminus \{0\}} I_p(C).$$

Proposition 2.1. *Let C be a convex subset of \mathbb{R}^2 containing 0 and with area less than $\frac{1}{2}$. Then the following holds:*

- i) *for any $v \in \mathbb{R}^2$, $I_v(C)$ is an interval in \mathbb{R} ;*
- ii) *for $p, p' \in \mathbb{Z}^2$, $I_p(C)$ and $I_{p'}(C)$ are contained in disjoint connected components of $R(C)$ if and only if p and p' are linearly independent;*
- iii) *there exists $\kappa > 0$ such that for any $v \in \mathbb{R}^2$ the distance between any two (successive) connected components of $I_v(C)$ is at least κ .*

Proof. i) If $g_tv, g_{t'}v \in C$ for $t < t' \in \mathbb{R}$, then $\{g_sv \mid t \leq s \leq t'\}$ is a segment of a hyperbola, and when C is a convex set containing 0 the segment is contained in C . This proves (i).

ii) Now let $p, p' \in \mathbb{Z}^2$ and suppose $I_p(C)$ and $I_{p'}(C)$ are contained in the same connected component of $R(C)$. Let $t \in I_p(C)$ and $t' \in I_{p'}(C)$ be given, with say $t < t'$; then t and t' are contained in the same connected component of $R(C)$. Since $R(C)$ is the union of intervals of the form $I_q(C)$, $q \in \mathbb{Z}^2 \setminus \{0\}$, t and t' being contained in the same connected component implies that there exist $p = p_0, p_1, \dots, p_{k-1}, p_k = p' \in \mathbb{Z}^2$ and $t = t_0 < t_1 < t_2 < \dots < t_k = t'$ such that $p_j \in g_s C$ for all $s \in [t_j, t_{j+1}]$ and $j = 0, \dots, k-1$. Consider any $1 \leq i \leq k$. We have $g_{t_j}^{-1}p_{j-1}, g_{t_j}^{-1}p_j \in C$, and hence

by the condition in the hypothesis the triangle with vertices at $g_{t_j}^{-1}p_{j-1}, g_{t_j}^{-1}p_j$ and 0 has area less than $\frac{1}{2}$. It follows that the triangle with vertices as p_{j-1}, p_j and 0 has area less than $\frac{1}{2}$. Since these vertices are integral points the conclusion implies that p_j and p_{j-1} are linearly dependent, for all $j = 1, \dots, k$. In particular we get that p and p' are linearly dependent.

Now suppose p, p' are linearly dependent, say $p = kp'$ with $k > 1$. Let $t \in I_p(C)$. Then there exists $v \in C$ such that $p = g_t(v)$. Then $p' = k^{-1}p = k^{-1}g_t(v) \in g_tC$, since $k^{-1} < 1$. This shows that I_p is contained in $I_{p'}$. In particular $I_p(C)$ and $I_{p'}(C)$ are contained in the same connected component of $R(C)$. This proves (ii).

iii) We can find a convex neighbourhood C' of C with area less than $\frac{1}{2}$. Then there exists a $\kappa > 0$ such that $g_tv \in C'$ for all $v \in C$ and $-\kappa \leq t \leq \kappa$. We see that each connected component of $R(C)$ are contained in a unique connected component of $R(C')$. Therefore the successive connected components of $R(C)$ are at a distance bounded below by κ . This proves (iii) \square

Proposition 2.2. *Let $Q = Q_g$ and $\theta > 0$ and $0 \leq r < r'$, be given. Let*

$$\Omega = \{v \in \mathbb{R}^2 \mid 0 < L_g^+(v) < \theta L_g^-(v) \text{ and } r < Q(v) < r'\} \text{ and } S = \Omega \cap \mathbb{Z}^2.$$

Let $\sigma \geq \sqrt{r'/\theta}$, and let

$$T = \{v \in \mathbb{R}^2 \mid 0 < L_g^+(v) < \theta L_g^-(v) \text{ and } 0 \leq L_g^-(v) \leq \sigma\}.$$

Suppose that T has area less than $\frac{1}{2}$. For $p \in S$ let $I_p = \{t \geq 0 \mid p \in g_t T\}$. Then each $I_p(T)$, $p \in S$, is nonempty, and for $\tau > \sigma$ any maximal set of pairwise linearly independent vectors contained in $\{p \in S \mid L_g^-(p) \leq \tau\}$ has cardinality equal to the number of connected components of $[0, 2 \log(\tau/\sigma)] \cap R(T \cap \Omega)$.

Proof. The assumption $\sigma \geq \sqrt{r'/\theta}$ ensures that the set of values of Q on the triangle T contain the interval $(0, r')$. This implies that for $p \in S$ there exists $v \in T$ and $t \geq 0$ such that $p = g_tv$, showing that $I_p(T)$ is nonempty.

Now, for $\tau > 0$ let $S(\tau) = \{p \in S \mid L_g^-(p) \leq \tau\}$. Now consider $\tau > \sigma$ and $p \in S(\tau)$. Then there exists $v \in T \cap \Omega$ with $L_g^-(v) = \sigma$ and $t > 0$ such that $p = g_tv$. Thus $L_g^-(p) = e^{t/2}L_g^-(v) = e^{t/2}\sigma$ and hence $t \leq 2 \log L_g^-(p)/\sigma \leq 2 \log(\tau/\sigma)$. Therefore for each $p \in S(\tau)$ there exists a $t \in [0, 2 \log(\tau/\sigma)]$ such that $p \in g_t(T \cap \Omega)$; let J_p denote the connected component of $[0, 2 \log(\tau/\sigma)] \cap R(T \cap \Omega)$ containing t . By Proposition 2.1 if $p, p' \in S(\tau)$ are linearly independent then $I_p(T)$ and $I_{p'}(T)$ belong to disjoint connected components of $R(T)$ and hence J_p and $J_{p'}$ are disjoint. This shows that the number of elements in any set of linearly independent vectors in $S(\tau)$ is bounded by the number of connected components of $[0, 2 \log(\tau/\sigma)] \cap R(T \cap \Omega)$.

Now let J be any connected component of $[0, 2 \log(\tau/\sigma)] \cap R(T \cap \Omega)$, and let $t \in J$. Then there exists $p \in \mathbb{Z}^2$ and $v \in T \cap \Omega$ such that $p = g_tv$. Clearly there exists

$t' \in J$ and $v' \in T \cap \Omega$ such that $L_g^-(v') = \sigma$ and $g_t(v) = g_{t'}(v')$, and hence by modifying notation we may assume that $L_g^-(v) = \sigma$. Hence $L_g^-(p) = e^{t/2}L_g^-(v) = e^{t/2}\sigma$. As $t \leq 2\log(\tau/\sigma)$, we get that $L_g^-(p) \leq \tau$ and hence $p \in S(\tau)$. Now suppose t and t' belong to different connected components, and let $p, p' \in S(\tau)$ be the elements obtained as above corresponding to t and t' respectively. Then $t \in I_p$ and $t' \in I_{p'}$. Thus $I_p(T)$ and $I_{p'}(T)$ are intervals containing respectively t and t' belonging to distinct connected components of $R(T \cap \Omega)$ and hence by Proposition 2.1 p and p' are linearly independent. This shows that there are at least as many mutually linearly independent vectors in $S(\tau)$ as the number of connected components of $[0, 2\log(\tau/\sigma)] \cap R(T \cap \Omega)$, which proves the proposition. \square

We denote by \mathfrak{p} the set of primitive integral pairs in \mathbb{Z}^2 , namely $p = xe_1 + ye_2 \in \mathbb{Z}^2$ such that $\gcd(x, y) = 1$. For any $\sigma > 0$ let

$$W(\sigma) = \{v = xe_1 + ye_2 \in \mathbb{R}^2 \mid 0 < y < x \leq \sigma\}.$$

For $\tau > \sigma > 0$ we denote by $n(\tau, \sigma)$ the the number of connected components of $\{t \in [0, 2\log(\tau/\sigma)] \mid ga_t W(\sigma) \cap \mathbb{Z}^2 \neq \emptyset\}$ or equivalently of the set of $t \in [0, 2\log(\tau/\sigma)]$ such that $a_{-t}\lambda \in W(\sigma)$, for some $\lambda \in \Lambda$, where $\Lambda := g^{-1}\mathbb{Z}^2$.

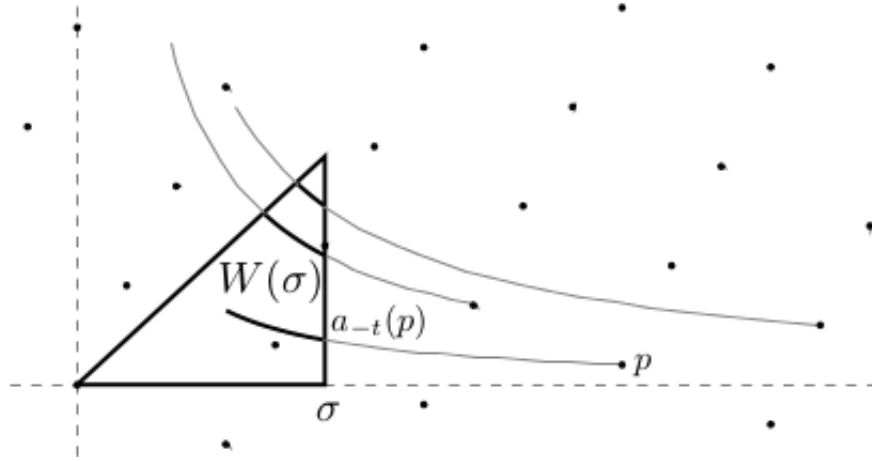


Figure 2: Trajectories passing through $W(\sigma)$

Corollary 2.3. *Let $Q = Q_g$. Let $0 < \epsilon < 1$ be given. For $\rho > 0$ let*

$$F(\rho) = \{p \in \mathfrak{p} \mid 0 < L_g^+(p) < L_g^-(p), 0 < Q(p) < \epsilon, \|p\| \leq \rho\}.$$

Then for all sufficiently large ρ the cardinality of $F(\rho)$ differs from $n(\|ge_1\|^{-1}\rho, \sqrt{\epsilon})$ by at most 1.

Proof. In Proposition 2.2 we choose $\theta = 1$, $r = 0$, $r' = \epsilon$, and let Ω and T be as in that Proposition. Then for the choices as above Ω contains T . Also, since $\epsilon < 1$ the area of T is less than $\frac{1}{2}$. We note also that in the above notation T coincides with $gW(\sqrt{\epsilon})$, and hence $g_t T = ga_t W(\sqrt{\epsilon})$. Then by Proposition 2.2, for any $\tau > \sqrt{\epsilon}$ the number of p in \mathfrak{p} such that $0 < L_g^+(p) < L_g^-(p) \leq \tau$ is $n(\tau, \sqrt{\epsilon})$. Let $\delta > 0$ be arbitrary. We note that for $v \in T$ and t sufficiently large

$$| \|g(e_1)\|^{-1} \|g_t(v)\| - L_g^-(g_t v) | < \delta.$$

Hence we get that for all large ρ the cardinality of $F(\rho)$ is bounded between $n(\|g(e_1)\|^{-1}\rho - \delta, \sqrt{\epsilon})$ and $n(\|g(e_1)\|^{-1}\rho + \delta, \sqrt{\epsilon})$. By Proposition 2.1 the successive connected components are at distance bounded below by a positive constant, and hence when δ is sufficiently small, for all large ρ , $n(\|g(e_1)\|^{-1}\rho + \delta, \sqrt{\epsilon})$ is at most one more than $n(\|g(e_1)\|^{-1}\rho - \delta, \sqrt{\epsilon})$. Hence the cardinality of $F(\rho)$ differs from $n(\|g(e_1)\|^{-1}\rho, \sqrt{\epsilon})$ by at most 1. This proves the corollary. \square

For $\delta > 0$ let B_δ be the open ball of radius δ in \mathbb{R}^2 , centered at 0, (in the usual metric) and let $B'_\delta = \{(x, y) \in B_\delta \mid 0 < y < x\}$.

Corollary 2.4. *Let $Q = Q_g$ and $0 < \delta < \frac{2}{\sqrt{\pi}}$ be given. Then for all sufficiently large $\rho > 0$ the cardinality of*

$$\{p \in \mathfrak{p} \mid 0 < L_g^+(p) \leq L_g^-(p), 0 < Q(p) < \frac{1}{2}\delta^2, \|p\| \leq \rho\}$$

differs from the number of connected components of $\{t \in [0, 2\log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t B'_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$ by at most 2.

Proof. In view of Corollary 2.3, for $\delta < 1$ the cardinality of the set under consideration differs by at most one from the number of connected components of $\{t \in [0, 2\log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t W(\delta/\sqrt{2}) \cap \mathbb{Z}^2\}$. Now, each of these connected components is contained in a connected component of $\{t \in [0, 2\log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$. Moreover when $\delta < \frac{2}{\sqrt{\pi}}$ the area of B'_δ is less than $\frac{1}{2}$, and hence by Proposition 2.1 distinct connected components of the former are contained in distinct connected components of the latter. Also, at most one connected component of $\{t \in [0, 2\log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$ can fail to intersect $\{t \in [0, 2\log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t W(\delta/\sqrt{2}) \cap \mathbb{Z}^2 \neq \emptyset\}$. The assertion as in the corollary is now immediate from these observations. \square

We shall say that two function f and f' on $(0, \infty)$ are *comparable* if the function $|f - f'|$ is bounded over $(0, \infty)$.

Corollary 2.5. *Let $Q = Q_g$ and $0 < \delta < \sqrt{\frac{2}{\pi}}$ and $\kappa > 0$ be given. For $\tau > 0$ let $c_g^+(\tau)$ and $c_g(\tau)$ denote, respectively, the number of connected components of $\{t \in [0, \tau] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$ and $\{t \in [-\tau, \tau] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$.*

i) for any $\rho > 0$ the cardinality of

$$G^+(\rho) = \{p \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, L_g^-(p) > \kappa, \|p\| \leq \rho\}$$

is comparable to $c_g^+(2 \log \rho)$.

ii) for any $\rho > 0$ the cardinality of

$$G(\rho) = \{p \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, \|p\| \leq \rho\}$$

is comparable to $2c_g(2 \log \rho)$.

Proof. i) The intersection of $G^+(\rho)$ with $\{v \in \mathbb{R}^2 \mid L_g^+(v) > 0\}$ differs from the set as in Corollary 2.4 by only a finite set (consisting of elements of \mathfrak{p} contained in the compact subset $\{v \in \mathbb{R}^2 \mid 0 \leq L_g^+(v) \leq L_g^-(v) \leq \kappa \text{ and } Q(v) \leq \frac{1}{2}\delta^2\}$) and hence by Corollary 2.4 the cardinality of $G^+(\rho)$ is comparable to the number of connected components of $\{t \in [0, 2 \log(\sqrt{2}\delta^{-1}\|ge_1\|^{-1}\rho)] \mid ga_t B'_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$. Since the distance between successive connected components is bounded below (by Proposition 2.1), the latter is comparable to the number of connected components of $\{t \in [0, 2 \log \rho] \mid ga_t B'_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$. Similarly we obtain that the cardinality of $G^+(\rho) \cap \{v \in \mathbb{R}^2 \mid L_g^+(v) < 0\}$ is comparable to the number of connected components of $\{t \in [0, 2 \log \rho] \mid ga_t B''_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$, where $B''_\delta = \{(x, y) \in B_\delta \mid 0 < -y < x\}$. We note that since $\delta < \sqrt{\frac{2}{\pi}}$ the area of the convex closure of $B'_\delta \cup B''_\delta$ is less than $\frac{1}{2}$ and hence the connected components of the sets $\{t \in [0, 2 \log \rho] \mid ga_t B'_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$ and $\{t \in [0, 2 \log \rho] \mid ga_t B''_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$ are disjoint from each other. Also, their union is the set of connected components of $\{t \in [0, 2 \log \rho] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$, except possibly for one connected component in the latter corresponding to a $p \in \mathfrak{p}$ such that $L_g^-(p) = 0$, in case L_g^- is a rational linear form. Hence the cardinality of $G^+(\rho)$ is asymptotic to $c_g^+(2 \log \rho)$. This proves assertion (i).

ii) Since when $p \in \mathfrak{p}$ belongs to $G(\rho)$ so does $-p$, from (i) we get also that the cardinality of $\{p \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, |L_g^-(p)| > \kappa, \|p\| \leq \rho\}$ is $2c_g^+(2 \log \rho)$.

Analogously, the set $\{p \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, |L_g^+(p)| > \kappa, \|p\| \leq \rho\}$ has cardinality comparable to the number of connected components of $\{t \in [-2 \log \rho, 0] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$. We note that $G(\rho)$ differs from $G^+(\rho) \cup G^-(\rho)$ by a fixed finite set. Therefore we get that the cardinality of $G(\rho)$ is comparable to $2c_g(2 \log \rho)$. This proves the corollary. \square

3 The geodesic flow and continued fraction expansions

We next relate the conclusion in Corollary 2.4 to the geodesic flow associated to the modular surface. The reader is referred to [3] for various general results on this topic

used in the sequel.

Let $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ be the Poincaré upper half plane. We view $\mathbb{R} \cup \{\infty\}$ as the boundary $\partial\mathbb{H}^2$ of \mathbb{H}^2 . We consider $\mathbb{H} \cup \partial\mathbb{H}^2$ equipped with the usual action of $G = SL(2, \mathbb{R})$. We recall that the geodesics $\{\varphi_t\}$ in \mathbb{H}^2 are Euclidean semicircles joining a pair of (distinct) points in $\mathbb{R} \cup \{\infty\}$, the boundary of \mathbb{H}^2 ; the two end points, say u and w , are the limits of $\{\varphi_t\}$ as $t \rightarrow -\infty$ and $t \rightarrow \infty$, and are respectively called the *repelling* and *attracting end points* of the geodesic; for simplicity we may identify the geodesic as the geodesic joining u and w .

Let K be the subgroup of G consisting of elements fixing i under the action on \mathbb{H}^2 , namely the elements of G acting as rotations on \mathbb{R}^2 . The G -action on \mathbb{H}^2 is transitive, and as such \mathbb{H}^2 can be realised as G/K . The geodesics in \mathbb{H}^2 then correspond to $\{ga_tK\}_{t \in \mathbb{R}}$, $g \in G$ (see [2], for instance), with the latter as the geodesic joining $g(0)$ and $g(\infty)$.

We denote by N the subgroup of G consisting of all upper triangular unipotent matrices. The orbits of the N -action on \mathbb{H}^2 consist of horizontal lines. We shall also use the notation $A = \{a_t \mid t \in \mathbb{R}\}$ and, for $\delta > 0$, $A_\delta = \{a_t \mid t < \log \delta\}$.

In the context of Corollary 2.5 we would be interested, for given $g \in G$, in solutions of $a_t^{-1}g^{-1}p \in B_\delta$ with $p \in \mathfrak{p}$ and $t \in \mathbb{R}$. Let $\Gamma = SL(2, \mathbb{Z})$. Then $\mathfrak{p} = \{\gamma e_1 \mid \gamma \in \Gamma\}$. Let $\gamma \in \Gamma$ be such that $p = \gamma e_1$. Then the condition as above translates to $a_t^{-1}g^{-1}\gamma e_1 \in B_\delta$ which is equivalent to $a_t^{-1}g^{-1}\gamma \in KA_\delta N$ and in turn to $\gamma^{-1}ga_t \in NA_\delta^{-1}K$, upon taking inverses. For $\delta > 0$ let $\mathbb{H}_\delta = \{x + iy \mid y > \delta^{-2}\}$. Then considering the G -action on \mathbb{H}^2 we see that the condition as above is equivalent to $\gamma^{-1}ga_t(i) \in \mathbb{H}_\delta$. Now consider the quotient map, say η , of \mathbb{H}^2 onto the “modular surface” $M = \Gamma \backslash \mathbb{H}^2$ and for $\delta > 0$ let $M_\delta = \eta(\mathbb{H}_\delta)$. Then the above condition is equivalent to $\eta(ga_t(i)) \in M_\delta$. Thus we see that

$$\{t \in \mathbb{R} \mid a_t^{-1}g^{-1}p \in B_\delta \text{ for some } p \in \mathfrak{p}\} = \{t \in \mathbb{R} \mid \eta(ga_t(i)) \in M_\delta\}. \quad (*)$$

Now $ga_t(i)$ is a geodesic in \mathbb{H}^2 and $\eta(ga_t(i))$ is its image under the quotient map (it is a geodesic with respect to the induced metric on M , but we will not need to go into the geometry on the quotient). The above observation enables us, using Corollary 2.4 on the one hand and coding of geodesics on the other hand to count the number of primitive solutions of quadratic inequalities in large balls in \mathbb{R}^2 .

Before proceeding with the main results we note the following:

Remark 3.1. If $g \in G$ and $Q = Q_g$, and if the inequality $|Q(p)| < \epsilon$ admits solutions $p \in \mathbb{Z}^2$ for all $\epsilon > 0$ then sets on the left hand side of $(*)$ have to be nonempty for all $\delta > 0$ (we shall not concern ourselves with the precise correspondence between the values here). Hence the observation shows in particular that if the image of the geodesic joining $g(0)$ and $g(\infty)$ under the quotient map onto the modular surface

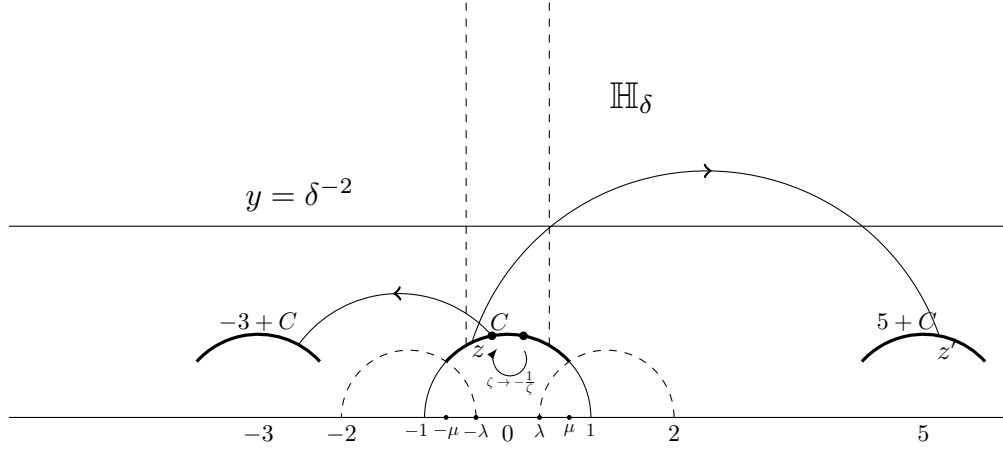


Figure 3: Segmentation of the geodesic trajectories

$M = \Gamma \backslash \mathbb{H}^2$ is bounded in M , then there exists $\epsilon > 0$ such that $|Q(p)| < \epsilon$ has no nonzero solution p in \mathbb{Z}^2 .

We now begin by introducing some notation, and recalling some definitions and facts about geodesics in \mathbb{H}^2 and their images in M .

Let $T^1(\mathbb{H}^2)$ be the unit tangent bundle of \mathbb{H}^2 , viewed as the set of pairs (z, ζ) with $z \in \mathbb{H}^2$ and ζ a unit tangent direction at z . For $(z, \zeta) \in T^1(\mathbb{H}^2)$ we denote by $\tilde{\varphi}(z, \zeta)$ the geodesic $\varphi = \{\varphi_t\}$ such that $\varphi_0 = z$ and ζ is the tangent direction to φ at z .

We recall, from Katok and Ugarcovici [3], that a geodesic $\varphi = \{\varphi_t\}$ in \mathbb{H}^2 with u and w the corresponding repelling and attracting endpoints in $\mathbb{R} \cup \{\infty\}$ is said to be *H-reduced* if $|w| > 2$ and $\text{sgn}(w)u \in [\lambda - 1, \lambda]$, where $\lambda = \frac{1}{2}(3 - \sqrt{5})$; in [3] the notation is r in place of the λ used here. Now let $\mu = (23 - 3\sqrt{5})/22$ and let C be the arc in \mathbb{H}^2 defined by

$$C = \{z = x + iy \in \mathbb{H}^2 \mid |z| = 1, |x| < \mu\}.$$

We note that μ chosen here is the x -coordinate of the point of intersection of the geodesic joining λ and 2 with $\{z \in \mathbb{H}^2 \mid |z| = 1\}$. It is straightforward to verify that for every *H-reduced* geodesic $\varphi = \{\varphi_t\}$ there exists a (unique) $t_0 \in \mathbb{R}$ such that $\varphi_{t_0} \in C$.

We shall be interested in the set of tangent vectors defined by

$$\Phi = \{(z, \zeta) \in T^1(\mathbb{H}^2) \mid z \in C, \tilde{\varphi}(z, \zeta) \text{ is } H\text{-reduced}\}.$$

We recall that every geodesic in \mathbb{H}^2 is equivalent, under the Γ -action, to a *H-reduced* geodesic [3]. Thus every geodesic in \mathbb{H}^2 is equivalent under the Γ action to (and hence has the same image in M as) a geodesic of the form $\tilde{\varphi}(z, \zeta)$, $(z, \zeta) \in \Phi$. It is known that Φ as above is a cross-section for the geodesic flow (see [3]), though it is

not stated in this form. We shall first give here a direct verification of this, together information on the return times that we will be using below.

Let $(z_0, \zeta_0) \in \Phi$ and $\varphi = \tilde{\varphi}(z_0, \zeta_0) = \{\varphi_t\}$ be the corresponding geodesic. Let u and w be the repelling and attracting endpoints of φ . We shall suppose that w is an irrational number. We now consider the (one sided) trajectory $\{\varphi_t\}_{t \geq 0}$, and divide it into segments as follows. Let $[a_0, a_1, \dots]$ be the minus continued fraction expansion of w following the Hurwitz algorithm.

We claim that the trajectory $\{\varphi_t\}_{t \geq 0}$ intersects the arc $\{a_0 + z \mid z \in C\}$, the translate of C at a_0 . Suppose first that $a_0 > 0$, so $a_0 \geq 2$; see Figure 3, for reference for the following argument, where a_0 is chosen to be 5. Since $w \in (a_0 - \frac{1}{2}, a_0 + \frac{1}{2})$, the trajectory $\{\varphi_t\}_{t \geq 0}$ intersects the semicircle $\{z \mid |z - a_0| = 1\}$; let z' be the point of intersection and let $\xi \in (-1, 1)$ be such that $a_0 + \xi$ is real part of z' . If $w > a_0$, which is in particular necessarily the case if $a_0 = 2$, then we have $\xi \leq \frac{1}{2} < \mu$ and hence $z' \in \{a_0 + z \mid z \in C\}$. We may therefore suppose that $a_0 \geq 3$ and $w < a_0$. We next observe that as $u \leq \lambda$ and $w > 2$, if ξ_0 is such that $a_0 + \xi_0$ is the point of intersection of the geodesic joining λ and $a_0 - \frac{1}{2}$ then $\xi_0 < \xi < 0$. A direct computation shows that $\xi_0 = \dots$. We deduce that $\xi_0 = -\mu$ if $a_0 = 3$ and if $a_0 > 3$ in fact $\xi_0 > -\mu$. This shows that z' is contained in $\{a_0 + z \mid z \in C\}$. Let ζ' be the unit tangent vector at z' , tangent to φ .

Now let $z_1 = -1/(z' - a_0)$, and ζ_1 be the tangent vector at z_1 , which is the image of the ζ' under the map $z \mapsto -1/(z - a_0)$. Then $z_1 \in C$, and we claim that $(z_1, \zeta_1) \in \Phi$, namely that $\tilde{\varphi}(z_1, \zeta_1)$ is H -reduced. Clearly the repelling and attracting endpoints of $\tilde{\varphi}(z_1, \zeta_1)$ are given by $u_1 = -1/(u - a_0)$ and $w_1 = -1/(w - a_0)$ respectively. Since $|w - a_0| < \frac{1}{2}$ we have $|w_1| = |1/(w - a_0)| > 2$, as required. Since $a_0 \geq 2$ and $u \leq \lambda < 1$, $u_1 = -1/(u - a_0)$ is positive, and we only need to confirm that the appropriate upper bounds hold for u_1 , depending on the sign of w_1 . If $w > a_0$ then $w_1 < 0$, and we have $u_1 = \frac{1}{a_0 - u} \leq \frac{1}{2 - \lambda} = 1 - \lambda$, and on the other hand if $w < a_0$ then $w_1 > 0$ and $a_0 \geq 3$, and in this case we have $u_1 = \frac{1}{a_0 - u} \leq \frac{1}{3 - \lambda} = \lambda$. Thus $(z_1, \zeta_1) \in \Phi$, which proves the claim.

Let $t_1 > 0$ be such that $\varphi_{t_1} = z'$, the latter being as above. We note also that for w_1 , which is the attracting endpoint of $\tilde{\varphi}(z_1, \zeta_1)$, the minus continued fraction is given by $[a_1, a_2, \dots]$. An analogous arguments works by symmetry with when $a_0 < 0$ and we get $(z_1, \zeta_1) \in \Phi$, and $t_1 > 0$ such that $z_1 = -1/\varphi_{t_1}$, ζ_1 is the image of the unit tangent to φ at φ_{t_1} under the corresponding map, and the attracting endpoint of $\tilde{\varphi}(z_1, \zeta_1)$, is given by $[a_1, a_2, \dots]$.

Repeating the procedure we get a sequence $\{(z_j, \zeta_j)\}$ in Φ and a sequence $\{t_j\}$ of positive numbers such that $z_j = -1/(\varphi_{t_j}(z_{j-1}) - a_{j-1})$ and the tangent to φ at $\varphi_{t_j}(z_{j-1})$ is mapped to ζ_j under the corresponding tangent map (in particular the pair $\varphi_{t_j}(z_{j-1})$ together with the unit tangent to φ at the point is equivalent to (z_j, ζ_j)

under the Γ action). Also, the attracting endpoints of $\tilde{\varphi}(z_j, \zeta_j)$ have the continued fraction expansion $[a_j, a_{j+1}, \dots]$, for all j .

We call $\{t_j\}$ as above the sequence of *return times* corresponding to the (z_0, ζ_0) or equivalently to the reduced geodesic $\varphi = \tilde{\varphi}(z_0, \zeta_0)$.

Now let $(z_0, \zeta_0) \in \Phi$, $\varphi = \tilde{\varphi}(z_0, \zeta_0)$, and ψ the image of φ under the quotient map $\eta : \mathbb{H}^2 \rightarrow M$. Let $\varphi = \{\varphi_t\}_{t \in \mathbb{R}}$; we equip ψ with the parametrization given by $\psi_t = \eta(\varphi_t)$ for all $t \in \mathbb{R}$. In the following we shall concern ourselves only with the (forward) trajectory $\{\psi_t\}_{t \geq 0}$. Using the return times of φ we divide the trajectory into parts $\psi^{(j)}$, $j \geq 0$; the indexing starting with 0 is chosen for notational convenience with respect to the related indices, as will be seen below. For each $j \geq 0$ let

$$\varphi^{(j)} = \{\tilde{\varphi}(z_j, \zeta_j)(t) \mid 0 \leq t < t_{j+1}\} \quad \text{and} \quad \psi^{(j)} = \eta(\varphi^{(j)}).$$

In the following propositions we collect properties of the segments $\varphi^{(j)}$ to be used in our counting results in the next section. In the following let $[a_0, a_1, \dots]$ be the minus continued fraction of the attracting endpoint of $\tilde{\varphi}(z_0, \zeta_0)$. Also let u_j and w_j be the repelling and attracting endpoints of $\tilde{\varphi}(z_j, \zeta_j)$.

Proposition 3.2. *Let $\delta \in (0, 1)$ and $j \geq 0$ be given. If $\varphi^{(j)} \cap \mathbb{H}_\delta \neq \emptyset$ then $|a_j| > 2\delta^{-2} + \lambda - \frac{3}{2}$, and if $|a_j| > 2\delta^{-2} + \lambda + \frac{1}{2}$ then $\varphi^{(j)} \cap \mathbb{H}_\delta \neq \emptyset$. When nonempty the intersection is an arc along the geodesic.*

Proof. We recall that $\varphi^{(j)}$ is the segment of the (euclidean) semicircle joining u_j and w_j lying between C and $a_j + C$ (both of which it intersects), and its intersection with \mathbb{H}_δ is the same as that of the semicircle; in particular, when nonempty it is an arc. Since $|w_j - a_j| < \frac{1}{2}$ and $\text{sgn}(w)u_j \in [\lambda - 1, \lambda]$ it follows that the radius of the circle is between $\frac{1}{2}(|a_j| - \frac{1}{2} - \lambda)$ and $\frac{1}{2}(|a_j| + \frac{1}{2} - (\lambda - 1))$. The assertion in the proposition is immediate from these observations. \square

Remark 3.3. In particular Proposition 3.2 shows that $\{\psi\}_{t \geq 0}$ is bounded (has compact closure) in M if and only if the sequence of partial quotients $\{a_j\}$ is bounded. Together with Remark 3.1 this shows that if $g \in G$ is such that $g(0)$ and $g(\infty)$ are irrational numbers whose minus continued fraction expansion with respect to the Hurwitz algorithm have bounded partial quotients then for $Q = Q_g$ the inequality $|Q(p)| < \epsilon$ has no nonzero solution for sufficiently small $\epsilon > 0$. We note also that this also shows, independently, that the partial quotients in the Hurwitz expansion of an irrational number are bounded if and only if the number is badly approximable in the usual sense.

Proposition 3.4. *Let $0 < \delta < 1$. Then for any $j \geq 0$ the arc $\varphi^{(j)} \cap \mathbb{H}_\delta$ (when nonempty) is a connected component of $\eta^{-1}(\psi^{(j)} \cap M_\delta)$. Moreover, if $\delta < (1 - \mu^2)^{1/4}$ then it is the only connected component of $\eta^{-1}(\psi^{(j)} \cap M_\delta)$ contained in \mathbb{H}_δ .*

Proof. For $\delta < 1$, for any $\gamma \in \Gamma$ which does not leave \mathbb{H}_δ invariant $\gamma\mathbb{H}_\delta$ is contained in $\{z = x + iy \in \mathbb{H}^2 \mid y < 1\}$. Hence the intersection of $\varphi^{(j)}$ with any such $\gamma\mathbb{H}_\delta$ is separated from $\varphi^{(j)} \cap \mathbb{H}_\delta$. This proves the first statement. If $\delta < (1 - \mu^2)^{1/4}$ then for any $\gamma \in \Gamma$ which does not leave \mathbb{H}_δ invariant $\gamma\mathbb{H}_\delta$ is contained in $\{z = x + iy \in \mathbb{H}^2 \mid y < \sqrt{1 - \mu^2}\}$. Since the endpoints of $\varphi^{(i)}$ have the y coordinates greater than $\sqrt{1 - \mu^2}$, $\varphi^{(i)}$ does not intersect $\gamma\mathbb{H}_\delta$ which is different from \mathbb{H}_δ . This completes the proof. \square

We shall denote by $d(z, z')$, where $z, z' \in \mathbb{H}^2$, the (hyperbolic) distance between z and z' in \mathbb{H}^2 . Let $\{\chi_j\}$ be the sequence of numbers defined by $\chi_j = \frac{1}{2} \log 3\sqrt{5}$ if $|a_j| \geq 3$ and $\chi_j = \log 2 - \frac{1}{2}d\left(\mu + i\sqrt{1 - \mu^2}, \frac{1}{2}(3 + i\sqrt{3})\right)$ if $|a_j| = 2$.

Proposition 3.5. $-2\chi_j \leq t_j - 2\log |a_j| \leq \log 3\sqrt{5} + \log\left(\frac{3}{4} + \sqrt{\frac{1}{2}}\right)$, for all $j \geq 0$.

Proof. Recall that each $\varphi^{(j)}$ is a geodesic segment joining a point of C to another on $a_j + C$, and t_j is its length. The distances of the initial point and the end point of the segment from i and $a_j + i$ respectively are bounded by $d(\mu + \sqrt{1 - \mu^2}, i)$, where, as before, $\mu = \frac{23-3\sqrt{5}}{22}$ is the x co-ordinate of the right endpoint of C . The latter distance is $\frac{1}{2} \log \frac{1+\mu}{1-\mu}$, and a numerical calculation shows that it equals $\frac{1}{2} \log 3\sqrt{5}$. Now let $d_j = d(i, a_j + i)$. Then from the above observations we get that

$$d_j - \log 3\sqrt{5} \leq t_j \leq d_j + \log 3\sqrt{5},$$

for all j . By a standard formula for distances in \mathbb{H}^2 (see [2]) we have

$$\begin{aligned} d_j &= \log\left(\frac{1}{2}|a_j^2| + \frac{1}{2}|a_j|\sqrt{|a_j|^2 + 4} + 1\right) \\ &= 2\log |a_j| + \log\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 + 4|a_j|^{-2}} + |a_j|^{-2}\right) \end{aligned}$$

and since $|a_j| \geq 2$ for all j the second term is (positive and) at most $\log\left(\frac{3}{4} + \sqrt{\frac{1}{2}}\right)$. Combining, we get that

$$-\log 3\sqrt{5} \leq t_j - 2\log |a_j| \leq \log 3\sqrt{5} + \log\left(\frac{3}{4} + \sqrt{\frac{1}{2}}\right),$$

for all $j \geq 0$. From the definition of χ_j 's we see that this proves the proposition in the case $|a_j| \geq 3$, and also the second inequality when $|a_j| = 2$.

It remains to prove the first inequality in the case when $|a_j| = 2$. For this we note that $\varphi^{(j)}$ is a segment joining a point of C to a point of $a_2 + C'$, where $C' = \{z = x + iy \in C \mid |x| \leq \frac{1}{2}\}$. It can be verified directly that the geodesic joining the endpoints $\mu + i\sqrt{1 - \mu^2}$ and $\frac{1}{2}(3 + i\sqrt{3})$ of C and $2 + C'$ is, along with its mirror image,

is the shortest of the segments as above. Thus $t_j \geq d\left(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+i\sqrt{3})\right)$. Hence

$$t_j - 2\log|a_j| \geq d\left(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+i\sqrt{3})\right) - 2\log 2 = -2\chi_j,$$

by the definition of χ_j when $|a_j| = 2$. \square

Remark 3.6. Let $\chi = \log 2 - \frac{1}{2}d\left(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+i\sqrt{3})\right)$, namely the value of χ_j when $|a_j| = 2$. We note that $\frac{1}{2}\log \frac{16}{11} \leq \chi \leq \frac{1}{2}\log \frac{3}{2}$. The semicircular geodesic segment joining $\frac{1}{2}(3+i\sqrt{3})$ to $\frac{3}{4} + i\frac{\sqrt{7}}{4}$ may be seen to be orthogonal to the unit circle at the latter point. Hence we have

$$d\left(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+i\sqrt{3})\right) \geq d\left(\frac{3}{4} + i\frac{\sqrt{7}}{4}, \frac{1}{2}(3+i\sqrt{3})\right).$$

By a direct computation we see that $d\left(\frac{3}{4} + i\frac{\sqrt{7}}{4}, \frac{1}{2}(3+i\sqrt{3})\right) = \log \frac{2+\sqrt{7}}{\sqrt{3}} \geq \log \frac{8}{3}$. Hence $\chi \leq \log 2 - \frac{1}{2}\log \frac{8}{3} = \frac{1}{2}\log \frac{3}{2}$. Also,

$$\begin{aligned} d\left(\frac{3}{4} + i\frac{\sqrt{7}}{4}, \mu + i\sqrt{1-\mu^2}\right) &= d\left(\frac{3}{4} + i\frac{\sqrt{7}}{4}, i\right) - d\left(\mu + i\sqrt{1-\mu^2}, i\right) \\ &= \log \sqrt{7} - \frac{1}{2}\log 3\sqrt{5}, \end{aligned}$$

from which we get that

$$d\left(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+i\sqrt{3})\right) \leq \log \frac{2+\sqrt{7}}{\sqrt{3}} + \log \sqrt{7} - \log \sqrt[4]{45} \leq \log \frac{11}{4},$$

as may be directly verified. Thus we have $\chi \geq \log 2 - \frac{1}{2}\log \frac{11}{4} = \frac{1}{2}\log \frac{16}{11}$.

4 Solutions of H -reduced quadratic inequalities

We say that an element $g \in G$ is H -reduced if the geodesic $\{ga_tK\}$ (under the identification as in § 3) is H -reduced. Now let $g \in G$ be such that $g(\infty)$ is an irrational number and let $Q = Q_g$; such a quadratic form may be called an *H -reduced quadratic form*. Let $[a_0, a_1, \dots]$ its minus continued fraction of $g(\infty)$ with respect to the Hurwitz algorithm. For all $n \in \mathbb{N}$ let

$$\alpha_n = \sum_{j=0}^{n-1} \log |a_j|.$$

Also for $\delta > 0$ and $n \in \mathbb{N}$ let

$$e(\delta, n) = \#\{0 \leq i \leq n-1 \mid |a_j| > 2\delta^{-2} + \frac{1}{2} + \lambda\} \text{ and}$$

$$f(\delta, n) = \#\{0 \leq i \leq n-1 \mid |a_j| > 2\delta^{-2} - \frac{3}{2} + \lambda\},$$

where, as in § 3, $\lambda = \frac{1}{2}(3 - \sqrt{5})$. Also let $c_0 = \frac{1}{2} \log 3\sqrt{5} + \frac{1}{2} \log \left(\frac{3}{4} + \sqrt{\frac{1}{2}}\right)$.

Theorem 4.1. *Let $0 < \delta < \sqrt{\frac{2}{\pi}}$ and $\kappa > 0$ be given, and for $\rho > 0$ let*

$$G(\rho) = \{p \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, L_g^-(p) > \kappa \text{ and } \|p\| \leq \rho\}.$$

There exist constants $\theta \geq 0$ and $\nu \in \mathbb{N}$ such that the following holds:

- i) if $\log \rho \geq \alpha_n + c_0 n + \theta$ then $\#G(\rho) \geq e(\delta, n) - \nu$, and*
- ii) if $\log \rho \leq \alpha_n - \omega_n - \theta$ then $\#G(\rho) \leq f(\delta, n) + \nu$.*

Proof. Let $\delta > 0$ be given. By Corollary 2.5, for any $\rho > 0$ the cardinality of $G(\rho)$ differs from $c_g^+(2 \log \rho)$ by a bounded amount, where $c_g^+(2 \log \rho)$ stands for the number of connected components of the set $\{t \in [0, 2 \log \rho] \mid ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset\}$. Hence it suffices to show that the estimates as in assertions (i) and (ii) hold for $c_g^+(2 \log \rho)$ (for the given δ , not included in the notation) in place of $\#G(\rho)$, with a ν' in place of ν .

We note that $t \geq 0$, $ga_t B_\delta \cap \mathbb{Z}^2 \neq \emptyset$ if and only if $a_t^{-1} g^{-1} \gamma \in B_\delta$ which, as seen in § 3, is equivalent to $\eta(ga_t(i)) \in M_\delta$. Note also that $\eta(ga_t(i)) = \psi_{t'+t}$ for all $t \in \mathbb{R}$. Hence $c_g^+(2 \log \rho)$ is the number of connected components of $\{t \in [0, 2 \log \rho] \mid \varphi_{t'+t} \in \mathbb{H}_\delta\}$.

Now let $(z, \zeta) \in \Phi$ be such that $\tilde{\varphi}(z, \zeta)$ is equivalent to the geodesic joining $g(0)$ and $g(\infty)$. Let $\varphi = \{\varphi_t\} = \tilde{\varphi}(z, \zeta)$. Let $\{t_j\}_{j=0}^\infty$ denote the corresponding sequence of return times (see § 3). Also let $t' \in \mathbb{R}$ be such that $g(i) = \varphi_{t'}$; such a t' exists since $g(i)$ is contained in the geodesic joining $g(0)$ and $g(\infty)$. We choose $\theta = |t'|$ and ν' to be the infimum of j such that $t_j \geq t'$. We show that assertions (i) and (ii) hold for these choices.

Now let ρ be as in (i), with $n \in \mathbb{N}$. Suppose first that $t' < 0$. Then

$$2 \log \rho \geq 2 \log \alpha_n + 2c_0 n - t' \geq \sum_{j=0}^{n-1} (2 \log |a_j| + 2c_0) - t' > \sum_{j=0}^{n-1} t_j - t'$$

and hence $c_g^+(2 \log \rho)$ contains $\{t \in [t_j, t_{j+1}) \mid \varphi_t \in \mathbb{H}_\delta\}$, for all $j = 0, \dots, n-1$. By Proposition 3.4 this implies $c_g^+(2 \log \rho)$ is at least as much as the number of $j \leq n-1$ for which $\varphi^{(j)}$ intersects \mathbb{H}_δ . By Proposition 3.2 this number is at least $e(\delta, n)$, which proves the claim in the case at hand. Now suppose that $t' \geq 0$. In this case the number of connected components of $c_g^+(2 \log \rho)$ is seen to be at least the number of those j 's for which $t_j > t'$ and $\varphi^{(j)}$ intersects \mathbb{H}_δ . By Proposition 3.2 the number of

$j \leq n-1$ for which $\varphi^{(j)}$ intersects \mathbb{H}_δ is at least $e(\delta, n)$. This shows that $c_g^+(2 \log \rho)$ is at least $e(\delta, n) - \nu$ which, as noted above, proves (i).

Next let ρ be as in (ii) with $n \in \mathbb{N}$. Then

$$2 \log \rho \leq 2 \log \alpha_n - \omega_n - t' \leq \sum_{j=0}^{n-1} (2 \log |a_j| - \chi_j) - t' < \sum_{j=0}^{n-1} t_j - t'.$$

Since $\sqrt{\frac{2}{\pi}} < (1 - \mu^2)^{1/4}$, by Proposition 3.4 this implies that $c_g^+(2 \log \rho)$ is at most the number of $j \leq n-1$ for which $\varphi^{(j)}$ intersects \mathbb{H}_δ , and Proposition 3.2 it is at most $f(\delta, n)$. This proves (ii). \square

5 Solutions of quadratic inequalities - the general case

Consider a binary quadratic form $Q(x, y)$, which is nondegenerate and not a scalar multiple of a form with rational coefficients. Then upto a scalar multiple Q is given by $Q(x, y) = (ay + bx)(cy + dx)$, for all $x, y \in \mathbb{R}$, where $ad - bc = 1$, $b \neq 0$ and $\frac{a}{b}$ is irrational. We shall therefore consider only forms Q satisfying these conditions on the coefficients. Thus $Q(x, y) = Q_g(xe_1 + ye_2)$, where $g = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix}$ is an element in G . We note that $g(\infty) = -\frac{a}{b}$, which by hypothesis is an irrational number. The element g may not be H -reduced, namely $\{ga_t K\}$ may not be a H -reduced geodesic. However it is equivalent under the action of Γ to an H -reduced geodesic. Thus there exists a $\gamma \in \Gamma$ such that $\{\gamma ga_t K\}$ is H -reduced. Let $g' = \gamma g$ and $Q' = Q_{g'}$; then g' is H -reduced, and we shall call Q' a *reduced version of Q* and γ an *H -reducing element* for Q .

We note that the factors L_g^+ and L_g^- of Q_g as introduced earlier are now given by $L_g^+(xe_1 + ye_2) = ay + bx$ and $L_g^-(xe_1 + ye_2) = cy + dx$, for all $x, y \in \mathbb{R}$. Let $L_{g'}^+$ and $L_{g'}^-$ be the corresponding linear forms for g' .

Let $[a_0, a_1, \dots]$ and $[a'_0, a'_1, \dots]$ be the minus continued fraction expansions of $\frac{a}{b}$ (which is irrational) and $g'(\infty)$ respectively. Since $g(\infty) = -\frac{a}{b}$, it follows that $[-a'_0, -a'_1, \dots]$ is the continued fraction expansion of $g(\infty)$. Since $g'(\infty) = \gamma g(\infty)$ we get also that there exists $m \in \mathbb{Z}$ such that $a'_j = -a_{j+m}$ for all large j . Now let

$$\alpha^+ = \limsup \frac{1}{n} \sum_{j=0}^{n-1} \log |a_j| = \limsup \frac{1}{n} \sum_{j=0}^{n-1} \log |a'_j|$$

and

$$\alpha^- = \liminf \frac{1}{n} \sum_{j=0}^{n-1} \log |a_j| = \liminf \frac{1}{n} \sum_{j=0}^{n-1} \log |a'_j|.$$

Let $\{\chi_j\}$ be the sequence, as before (defined by $\chi_j = \frac{1}{2} \log 3\sqrt{5}$ if $|a_j| > 2$ and $\chi_j = \log 2 - \frac{1}{2}d(\mu + i\sqrt{1-\mu^2}, \frac{1}{2}(3+\sqrt{3}))$ if $|a_j| = 2$) and let

$$\omega_n = \sum_{j=0}^{n-1} (\log |a_j| - \chi_j) \text{ for all } n \in \mathbb{N}, \text{ and } \omega = \liminf \frac{1}{n} \omega_n.$$

It may be borne in mind that each of α^+, α^- and ω can be infinite. On the other hand $\alpha^+ \geq \alpha^- \geq \log 2$. Also, as

$$\log 2 - \chi \geq \log 2 - \frac{1}{2} \log \frac{3}{2} > \log 3 - \frac{1}{2} \log 3\sqrt{5} = \frac{1}{4} \log \frac{9}{5},$$

we have $\log |a_j| - \chi_j \geq \frac{1}{4} \log \frac{9}{5}$ for all j , and hence $\omega \geq \frac{1}{4} \log \frac{9}{5}$. We note also that similarly $\omega \geq \eta \alpha^-$, where $\eta = (\log \frac{9}{5}) / (4 \log 3) > \frac{1}{8}$.

Also, for any $\delta > 0$ let

$$e^-(\delta) = \liminf_{n \rightarrow \infty} \frac{1}{n} e(\delta, n), \quad e^+(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} e(\delta, n)$$

$$f^-(\delta) = \liminf_{n \rightarrow \infty} \frac{1}{n} f(\delta, n) \text{ and } f^+(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} f(\delta, n).$$

We note that $\alpha^+, \alpha^-, \omega, e^+(\delta)$ and $e^-(\delta)$ are determined by $\{a_j\}$, and hence by $\frac{a}{b}$.

Corollary 5.1. *Let Q be a binary quadratic form, as above, given by $Q(x, y) = (ay+bx)(cy+dx)$, for all $x, y \in \mathbb{R}$, where $ad-bc = 1$, $b \neq 0$ and $\frac{a}{b}$ is irrational. Let the notation $\alpha^+, \omega, e^+(\delta)$ and $e^-(\delta)$ be as above, and let $c_0 = \frac{1}{2} \left(\log 3\sqrt{5} + \log(\frac{3}{4} + \sqrt{\frac{1}{2}}) \right)$, as before. Let $0 < \delta < \sqrt{\frac{2}{\pi}}$ and $\kappa > 0$ be given, and for any ρ let*

$$G(\rho) = \{p = xe_1 + ye_2 \in \mathfrak{p} \mid 0 < |Q(p)| < \frac{1}{2}\delta^2, \quad cy + dx > \kappa \text{ and } \|p\| \leq \rho\}.$$

Let $\epsilon > 0$ be arbitrary. Then we have the following:

i) if $\alpha^+ < \infty$ then there exists ρ_0 such that for all $\rho \geq \rho_0$ we have

$$\#G(\rho) \geq (1 - \epsilon) \frac{e^-(\delta)}{(\alpha^+ + c_0)} \log \rho;$$

ii) given $0 < M \leq \omega$ there exists ρ_0 such that for all $\rho \geq \rho_0$ we have

$$\#G(\rho) \leq (1 + \epsilon) \frac{f^+(\delta) + \epsilon}{M} \log \rho.$$

In particular this holds for all $0 < M \leq \eta \alpha^-$.

Proof. Let $\gamma \in \Gamma$ be an H -reducing element for Q , $g' = \gamma g$ and $Q' = Q_{g'}$. For any $\rho > 0$ let $G'(\rho) = \{p \in \mathfrak{p} \mid 0 < Q'(p) < \delta^2, L_{g'}^-(p) > \kappa \text{ and } \|p\| \leq \rho\}$. Then we have $Q(p) = Q'(\gamma p)$ and $L_g^-(p) = L_{g'}^-(\gamma p)$ for all $p \in \mathbb{Z}^2$, and hence $\#G'(\|\gamma\|^{-1}\rho) \leq \#G(\rho) \leq \#G'(\|\gamma\|\rho)$ for all $\rho > 0$, where $\|\gamma\|$ denotes the operator norm of γ (as an element of G). This shows that it suffices to prove the assertions in the corollary with $G'(\rho)$ in place of $G(\rho)$, namely in the case when γ is the identity element. In other words we may assume, as we shall, that g is H -reduced.

Let θ and ν be as in Theorem 4.1. Let $v = \sqrt{1 + \epsilon}$. There exists n_0 such that for all $n \geq n_0$ we have $e(\delta, n) - \nu \geq v^{-1}e^-(\delta)n$ and $\alpha_{n+1} + c_0(n+1) + \theta \leq v(\alpha^+ + c_0)n$. Let $\rho_0 > 0$ be such that $\log \rho_0 = \alpha_{n_0} + c_0 n_0 + \theta$. Consider $\rho \geq \rho_0$. Then there exists $n \geq n_0$ such that $\alpha_n + c_0 n + \theta \leq \log \rho \leq \alpha_{n+1} + c_0(n+1) + \theta$. Then by Theorem 4.1 we have $\#G(\rho) \geq e(\delta, n) - \nu \geq v^{-1}e^-(\delta)n$. Also by choice $\log \rho \leq \alpha_{n+1} + c_0(n+1) + \theta \leq v(\alpha^+ + c_0)n$, and hence $n \geq \log \rho / v(\alpha^+ + c_0)$. Thus we get that

$$\#G(\rho) \geq v^{-2} \frac{e^-(\delta)}{(\alpha^+ + c_0)} \log \rho \geq (1 - \epsilon) \frac{e^-(\delta)}{(\alpha^+ + c_0)} \log \rho,$$

which proves (i).

Next we choose n_0 such that for all $n \geq n_0$ we have $f(\delta, n) + \nu \leq v(f^+(\delta) + \epsilon)n$ and $\omega_{n-1} - \theta \geq v^{-1}Mn$. Let $\rho_0 > 0$ be such that $\log \rho_0 = \omega_{n_0} - \theta$, and consider $\rho \geq \rho_0$. Since $\omega > 0$, $\omega_n \rightarrow \infty$ and hence there exists $n \geq n_0 + 1$ such that $\log \rho \leq \omega_n - \theta$; we pick the least integer $n \geq n_0 + 1$ with this property, so $\log \rho \geq \omega_{n-1} - \theta$. By Theorem 4.1 we have $\#G(\rho) \leq f(\delta, n) + \nu \leq v(f^+(\delta) + \epsilon)n$. Also since $\log \rho \geq \omega_{n-1} - \theta \geq v^{-1}Mn$, we get that $n \leq \frac{v}{M} \log \rho$. This yields

$$\#G(\rho) \leq v^2 \frac{f^+(\delta) + \epsilon}{M} \log \rho = (1 + \epsilon) \frac{f^+(\delta) + \epsilon}{M} \log \rho,$$

which proves (ii). \square

Proof of Theorem 1.1: The theorem follows from Corollary 5.1 when we interchange the role of x and y and replace δ by $\sqrt{2\delta}$; we note that $e(\delta)$ and $f(\delta)$ as in Theorem 1.1 are respectively at most and at least as much as the corresponding constants in Corollary 5.1, since $\lambda < \frac{1}{2}$. \square

The following special case may be worth emphasizing, on account of its comparability with the fact that if $[a_0, a_1, \dots]$ is bounded then for sufficiently small $\delta > 0$ the set of solutions $G(\rho)$ as above is empty.

Corollary 5.2. *Let the notation be as above. If $f^+(\delta) = 0$ then*

$$\lim_{\rho \rightarrow \infty} \frac{\#G(\rho)}{\log \rho} = 0;$$

in particular, if S is a subset of \mathbb{N} with zero upper density and $\{a_j\}$ is bounded on the complement of S , then this conclusion holds, for all sufficiently small $\delta > 0$.

Proof. The proof is immediate from Corollary 5.1. □

Acknowledgement: The authors are thankful to the referee for suggestions leading to improvement of the presentation of the paper. The authors are also thankful to L. Singhal for his help in drawing the figures included in this paper.

References

- [1] Manfred Einsiedler and Thomas Ward, *Ergodic theory with a view towards number theory*, Graduate Texts in Mathematics, 259. Springer-Verlag London, Ltd., London, 2011. xviii+481 pp.
- [2] Svetlana Katok, *Fuchsian groups*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1992. x+175 pp.
- [3] Svetlana Katok and Ilie Ugarcovici, Arithmetic coding of geodesics on the modular surface via continued fractions, *European women in mathematics* XMarseille 2003, 59V77, CWI Tract, 135, Centrum Wisk. Inform., Amsterdam, 2005.
- [4] Svetlana Katok and Ilie Ugarcovici, Symbolic dynamics for the modular surface and beyond, *Bull. Amer. Math. Soc.* 44 (2007), 87-132.
- [5] G.A. Margulis, Oppenheim conjecture, *Fields Medallists' lectures*, 272 - 327, World Sci. Ser. 20th Century Math., 5, World Sci. Publ., River Edge, NJ, 1997.

Manoj Choudhuri
Centre for Applicable Mathematics
Tata Institute of Fundamental Research
Yelahanka, Bangalore 560065, India.
manoj@math.tifrbng.res.in

S.G. Dani
Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India.
sdani@math.iitb.ac.in